

New protection in the face of new threats



Alfonso XI, 'the Avenger', was a Spanish king who once described in awe how during a battle against the Marinids, "they hurled many iron balls with thunder and the Christians were deeply afraid, as any man's limb that was hit was sliced off as if with a knife".

He was describing the impact of gunpowder on his troops. Soldiers, for whom in 14th century a battle meant swords, shields and arrows, were suddenly confronted with a new weapon that rendered their 'security technology' utterly useless.

It was a similar story when the Mark I tank entered into action in the battle of the Somme in 1916. The trench defenses prepared to repel soldiers offered scant resistance, and the bullets from soldiers' rifles just bounced off the tank's metal shell. Once again, there was no technology available to confront the new threat.

And away from the theatre of war, human beings have faced many situations in which our concept of security has had to adapt: What use were the handkerchiefs people wore around their faces to keep Spanish flu at bay in 1918? None whatsoever: the virus causing the flu was so small that no handkerchief could filter it out. Special filters had to be developed to protect against airborne viruses.

And today we also face similar problems with security systems, in this case, IT security. In the early days of personal computing, the emergence of viruses exposed users to a new threat for which they were ill-prepared. Existing technology was of no use and programs had to be developed to stop viruses: antivirus programs.

Shortly however, more advanced protection was needed. There were more and more viruses, and security laboratories were hard pushed to generate all the necessary vaccines. In the war that was being waged, the quality of the malware was practically irrelevant, the strategy was to saturate the antivirus developers. Whereas previously just a couple of dozen viruses a day were detected, now hundreds if not thousands were appearing.

Proactive detection technologies, designed to root out new malicious code, fulfill their purpose, but once again new weapons are being used that can breach even proactive defenses (and even these are only developed by a select few security companies).

Many businesses (and also home computers) have seen an upsurge in targeted attacks by hackers. Software using special stealth techniques (e.g. rootkits), unique creations targeted at a single computer with vital

New protection in the face of new threats



information... these are the new weapons. The 'business opportunities' of having, say, a Trojan spying on competitors are such that hackers are now renouncing the lure of personal notoriety in favor of cash rewards.

While these attacks surreptitiously harvest confidential information, new examples of malware still pour into security laboratories. It's just like a scene from an epic war film: hundreds or thousands of soldiers charge into action, sacrificed for the cause, while on a distant hilltop the general watches as the special-forces secretly penetrate enemy lines.

The technology needs to be reinvented. The reactive technologies of the classic resident antivirus are simply not enough. The panorama has changed, and the protection strategy must also change. Outdated technologies are about as useful as a mediaeval shield against an assault rifle.

Today, in the time it takes a lab technician to start up a computer to investigate a malicious code, an infection can spread massively. The record-holder in this field is SQLSlammer, which some sources claim took just 15 seconds.

To establish a protection system against new threats, we need to set up an intelligent layer of protection in every system connected to the Internet, be it a corporate workstation or a home PC. This means a system that can analyze what is happening on a computer and detect dangerous behavior, stopping it before it is too late.

This type of technology for detecting unknown threats (and I'm not speaking about classic heuristics systems, but intelligent technologies) are readily available from some manufacturers of consumer security solutions. But where is the protection for corporate networks? Why should administrators with hundreds or thousands of computers have to go without protection against unknown threats?

Fernando de la Cuadra
International Technical Editor
Panda Software (<http://www.pandasoftware.com>)
E-mail: Fdelacuadra@pandasoftware.com